AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the above-identified application:

1. (Currently Amended) An electronic device including an autonomous memory checker for runtime security assurance, the electronic device comprising:

a controller adapted to fetch first memory content from a portion of memory, wherein the first memory content includes software executable on the electronic device;

a memory reference file coupled to said controller, and adapted to store at least one memory reference value that corresponds to the first memory content; and

an authentication engine coupled to said controller, and adapted to perform ~~wherein~~ a runtime check ~~is performed~~ during runtime operation of the electronic device by comparing a ~~real-time~~ at least one runtime reference value with the at least one memory reference value, wherein the at least one runtime reference value corresponds to second memory content fetched from the portion of memory during the runtime operation of the electronic device ~~corresponding to information stored in memory to a memory reference value~~.

2. (Original) The electronic device as recited in claim 1 wherein said check is performed periodically during runtime operation of the electronic device.

3. (Original) The electronic device as recited in claim 1 wherein said check is performed at random times during runtime operation of the electronic device.

4. (Original) The electronic device as recited in claim 1 further including a clock control block coupled to said authentication engine, said memory reference file, and said controller.

5. (Original) The electronic device as recited in claim 4 further including a direct memory access (DMA) controller coupled to said authentication engine and said controller.

6. (Original) The electronic device as recited in claim 5 further including a timing module coupled to said controller.

7. (Currently Amended) The electronic device as recited in claim 1 wherein said memory content includes trusted information stored in the memory, and wherein said memory reference value is generated corresponding to the trusted information stored in the memory ~~and wherein said memory reference value is stored in said memory reference file~~.

8. (Original) The electronic device as recited in claim 7 wherein said trusted information stored in memory is processed by said authentication engine to generate said memory reference value.

9. (Original) The electronic device as recited in claim 8 wherein said information stored in memory is processed by said authentication engine to generate said real-time reference value, and wherein said information stored in memory has not been modified if said memory reference value is identical to said real-time reference value.

10. (Currently Amended) A method of operating an electronic device for runtime security assurance comprising the steps of:

storing trusted information in specific memory locations within a memory of the electronic device, wherein the trusted information includes software executable on the electronic device;

fetching said trusted information from the specific memory locations, and providing said trusted information to an authentication engine;

generating a memory reference value corresponding to said trusted information fetched from the specific memory locations;

storing said memory reference value in a memory reference file;

operating the electronic device in a runtime mode of operation;

fetching memory content from the specific memory locations, and providing the memory content corresponding to the specific memory locations ~~where said trusted information was stored~~ to said authentication engine during the runtime mode of operation of the electronic device;

generating a ~~real-time~~ runtime reference value from the memory content fetched from the specific memory locations; and

comparing said ~~real-time~~ runtime reference value to said memory reference value.

11. (Original) The method as recited in claim 10 wherein said step of generating a memory reference value corresponding to said trusted information further includes a step of generating said reference value with a hardware authentication engine.

12. (Currently Amended) The method as recited in claim 10 further including the steps of:

continuing the runtime mode of operation of the electronic device when said ~~real-time~~ runtime reference value is identical to said memory reference value; and

signaling an error when said ~~real-time~~ runtime reference value is not identical to said memory reference value.

13. (Currently Amended) The method as recited in claim 12 further including a step of repeating a runtime check process comprising the steps of again fetching memory content from the specific memory locations, generating a ~~real-time~~ another runtime reference value from memory content, ~~corresponding to memory locations where said trusted information was stored~~ and comparing said ~~real-time~~ another runtime reference value to said memory reference value.

14. (Currently Amended) The method as recited in claim 13 further including a step of running said runtime check process in a background of the runtime mode of operation of the electronic device.

15. (Currently Amended) The method as recited in claim 14 further including a step of randomizing when said runtime check process occurs during the runtime mode operation of the electronic device.

16. (Currently Amended) A method of operating an electronic device for runtime security assurance comprising the steps of:

fetching trusted information from a portion of memory of the electronic device, wherein the trusted information includes software executable on the electronic device;

providing the trusted information ~~stored in memory to be hashed~~ to an autonomous memory checker during a boot-time ~~boot~~ mode of operation of the electronic device;

instructing said autonomous memory checker to hash said trusted information during said boot-time ~~boot~~ mode;

generating, by said autonomous memory checker, reference hash values from said trusted information;

storing said reference hash values to a memory reference file ~~within said autonomous memory checker~~;

fetching, during a runtime mode of operation of the electronic device, memory contents from the portion of memory from which said trusted information was previously fetched ~~from memory during runtime for hashing by said autonomous memory checker~~;

generating, by said autonomous memory checker, runtime hash values with said ~~trusted information~~ memory contents retrieved during the runtime mode;

comparing said reference hash values to said runtime hash values; and

signaling an error when said reference hash values differ from said runtime hash values to indicate that said trusted information has been modified.

17. (Currently Amended) The method as recited in claim 16 further including a step of repeating randomly the steps of:

fetching, during the runtime mode, the memory contents from the portion of memory from which said trusted information was previously fetched ~~from memory during runtime for hashing by said autonomous memory checker~~;

generating, by said autonomous memory checker, the runtime hash values with said ~~trusted information~~ memory contents retrieved during the runtime mode;

comparing said reference hash values to said runtime hash values; and

signaling [[an]] the error when said reference hash values differ from said runtime hash values to indicate that said trusted information has been modified.

18. (Currently Amended) The method as recited in claim 16 wherein said step of fetching the trusted information from the portion of memory ~~providing trusted information stored in memory to be hashed to an autonomous memory checker during a boot mode~~ includes a step of fetching said trusted information from a plurality of memory blocks.

19. (Original) The method as recited in claim 18 further including a step of continuing runtime operation of the electronic device when said runtime hash values are identical to said reference hash values.

20. (New) The electronic device as recited in claim 1, wherein the controller is a bus master that is allowed to fetch the memory content from memory without requesting permission.